RC Technologies

Customer Proprietary Network Information
Compliance Manual & Operating Procedures

TABLE OF CONTENTS

What is CPNI?

CPNI is defined as (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, and (B) information contained in the bills pertaining to telephone exchange service or telephone toll received by a customer of a carrier or Internet services provided.

Practically speaking, CPNI includes information such as the phone numbers called by a consumer, the frequency, duration and timing of such calls; and any services purchased by the consumer, such as call waiting.

What is not CPNI?

Subscriber list information – name, address and telephone number; information from non-telecommunications services, cable TV.

When may a carrier use, disclose or permit access to a customer's CPNI without customer approval?

- As required by law
- To discuss the customer's existing services
- To answer any questions the customer has about any charges on his/her bill once the customer had been validated.
- To provision or market inside-wire installation, maintenance or repair service
- To market an improvement/enhancement or additional services among the category of services to which the customer already subscribes. For example, if a customer subscribes to local and long distance services, a carrier can market custom calling features, call blocking, toll plans, internet service, etc.
- To provision CPE and call answering, voice mail or messaging, voice storage and retrieval services, and fax store and forward

When must a carrier have customer approval to use CPNI?

- To use CPNI to market a service outside the customer's existing service relationship
- To share CPNI with a third party

NOTE: Customers have a right to obtain access to, and compel disclosure of, their own CPNI. Specifically, every telecommunications carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."

RC's Method for obtaining customer approval

Opt-out approval:

- Notification is provided to customer and if the customer doesn't object within the waiting period (30-day minimum period), customer is deemed to have consented to the use of his/her CPNI
- Must provide notification every two years

Carrier Authentication Requirement

A carrier MUST authenticate a customer (the person listed on the account) before discussing any account information. Do this by asking the authentication question determined by the carrier. If the husband is listed on the account, a carrier should not be discussing CPNI with the wife if she is not listed on the account. Another instance could be when a son or daughter handles his/her parent's account, but they are not listed on the account.

The type of CPNI being accessed determines the type of authentication. The two types of CPNI are defined below:

- "Call detail" information defined as any information that pertains to the transmission of specific telephone calls, e.g., number called or number from which call was placed, time, location and duration of call
- "Non-call detail" information, e.g., products, types of services customer subscribes to, technical configuration

Carriers can only release "call detail" information as follows:

- Customers that come into the office must provide a valid photo ID (e.g., government-issued personal identification with a photograph such as a current driver's license, passport, or comparable ID)
- Carrier can send the call detail information to the customer's address of record
- Carrier can call the telephone number of record and disclose call detail information

The carrier may not disclose to the customer or discuss with the customer any call detail information about the customer account other than the call detail information the customer provides. (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call.)

Online account access

Must have password protection for all CPNI available online to the customer, not just for "call detail" information.

NOTE: There is an exception for business customers – if the carrier's contract with a business customer is serviced by a dedicated account representative as the primary contact, and specifically addresses the carrier's protection of CPNI, the carrier authentication rules do not apply.

Notification of Account Changes

- The carrier must notify customers immediately of certain account changes, including whenever customer response to authentication question, online account, or address of record is created or changed. (This is not required when the customer initiates service)
- Notification to the customer must not reveal the changed account information

- The carrier may not notify customer of account changes by sending notice to the new account information (e.g., mailing a customer's change of address notification to a new address rather than to the former address of record.)
- Notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record

Notice of Unauthorized Disclosure (Breach) of CPNI

- A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI
- As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The FCC will maintain a line to the reporting facility at http://www.fcc.gov/eb/cpni
- Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI unless:
  -the carrier believes there is an extraordinarily urgent need to notify any class of affected customers sooner, than otherwise allowed under paragraph (b)(1) of this section, in order to avoid immediate and irreparable harm, it shall so indicated in its notification and may proceed to immediately notify its affected customer only after consultation with the relevant investigating agency.
  -the USSS or FBI requests an extension that cannot be more than 30 days for the initial request.
- Carrier shall maintain a record of any breach and the notification for a minimum of two (2) years

Annual Certification Filing

- Carriers must file their annual certification with the FCC on, or before, March 1 for data pertaining to the previous calendar year
- Certification must be executed by an officer of the carrier
- Officer must state that he/she has "personal knowledge" that the carrier has established procedures adequate to ensure compliance with the CPNI rules
- Must provide an accompanying statement explaining how the carrier's procedures ensure that the carrier is or is not in compliance with the requirement
- Must include an explanation of any actions taken against data brokers
- Must include a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI

Employee Disciplinary Procedures

Unintentional disclosure or violation of the company's CPNI rules will result in the following:

- Reprimand
- Retrain
- Re-certification

- Escalated disciplinary actions for repeat offenses

Intentional distribution of CPNI to other parties to harm the company or for personal gain will result in the following:

- Termination

CUSTOMER CARE CONSULTANT GUIDELINES

Before a customer care consultant (CCC) can handle customer calls or in-office visits, the CCC will need to know the following:

- **Has the company asked customers for permission to use CPNI?** If yes, where is the status of the customer's CPNI approval noted in the customers' records?

- **How is the company going to handle call detail information for customer-initiated calls?** Have they assigned passwords or are they going to provide call-detail information by one of the other acceptable methods?

- **What type of authentication has the carrier decided to use for non-call detail information?** Where is it noted in the customers' records?

- **Understand the following things can be discussed <u>without</u> customer approval:**
  - Customer's existing services.
  - An improvement/enhancement to an existing service.
  - Questions customer has about charges on bill.
  - CPE provisioning.
  - Inside wire installation, maintenance or repair service.

- **If the CCC determines that to proceed with the call, approval is needed to use the customer's CPNI for the duration of the call, the CCC must provide the customer verbal notification and ask for approval.** (Not required if the customer has previously given approval via the opt-in or opt-out methods.)

  Example: Permission is needed if the customer wants to discuss service offerings outside of the customer's existing company-customer relationship. (Customer subscribes to local and your long distance and wants to talk about wireless.)

  NOTE: If you are billing toll for another carrier, you <u>cannot</u> use that CPNI to market your own toll.

  If in doubt as to whether or not you will need permission, it is better to ask for permission to look at the customer's CPNI.

  Following is suggested script for a one-time use of CPNI:

  The FCC has adopted rules to protect the privacy of telecommunications information that is personal to you and that is available to our company because of our company-customer relationship. That information would include the

services you subscribe to, the amount of usage of those services, and other information you have provided to us. Under federal law, we have a responsibility to protect your data and you have a right to protect the confidentiality of your account information. We need your permission to access your account information. If you give us permission, it will be for the duration of this call only. Do we have your permission?

In-Office Customer Visit

Step 1: Authenticate the customer with a valid photo ID and confirm that the person is listed as a contact on the account.
Step 2: Check status of customer's CPNI approval.
Step 3: Respond to the customer's request following the rules for whether or not CPNI approval is needed.

NOTE:

If the customer is just dropping off payment, no authentication is needed unless the customer needs to know the amount of the bill.

If the person paying the bill is not listed on the account, the company cannot disclose the amount due. The person would need to tell the company the amount that the customer wanted to pay on the account.

Customer-Initiated Call

Step 1: Authenticate the customer (authentication question) and confirm the customer is listed as a contact on the account.
Step 2: Check status of the customer's CPNI approval.
Step 3: Respond to the customer's request following the rules for whether or not CPNI approval is needed.

The company has made the decision not to issue passwords. A customer calls the office, and an answer to the authentication question has not been previously established. How should this be handled?

Apologize to the customer for the inconvenience. Explain to the customer, that to protect the customer's privacy, the FCC now requires the company to authenticate the customer before discussing any information in the account.

Since this does not involve authentication for a password, the CCC could do one of the following:

- Call the customer at the telephone number of record.
- Ask the customer to provide some information contained in the account, e.g., services the customer subscribes to, amount of last bill, other names listed on the account, etc.

Once the CCC has authenticated the customer, explain that whenever the customer calls the office in the future, you will ask them for the answer to a specific question that you are now going to ask. You will then need to ask the question and record the answer in the customer's account records.

The company has made the decision <u>not</u> to issue passwords. What if a customer calls into the office and wants to discuss call detail on the bill?

If the customer is able to provide all of the call detail information (e.g., telephone number called, when it was called and the amount of the call) necessary to address the customer's issue, the company is permitted to handle the customer's inquiry.

If the customer cannot provide the call detail information or wants to know all of the toll charges listed on the bill, the carrier must do one of the following:

- Call the telephone number of record.
- Send the call detail information to the address of record.
- Ask the customer to come into the office and provide valid photo ID.

What if the person that comes into the office or calls the office is not listed on the account?

The CCC should explain that he/she is sorry for the inconvenience, but the FCC rules for protecting a customer's account information allow you to speak only with a person listed on the account. You can explain that the person listed on the account will need to call the company or come into the office and authorize adding an additional name to the account.

What if a person calls into the office and has the password, or answer to the authentication question, but is not listed on the account? Is that enough?

No, the person must be listed on the account as an authorized contact.

What if a woman calls in and says she is John Doe and has the answer to the authentication question for the account, do we care that she is a woman and not "John"?

Yes, if you know you are talking to a woman and the person listed on the account is a man, you cannot discuss the account.

Of course, you'll need to be careful in these instances if you don't know the person listed on the account. Many of the same names are used for both male and female.

QUESTIONS AND ANSWERS

Does a company need to authenticate every customer?
Yes, if the customer calls the office or comes into the office, the customer must be authenticated.

Can the company rely on Caller ID to authenticate the customer?
No, because a pretexter can easily manipulate or replicate this information.

Does a company need to assign passwords?
No, the FCC does not mandate passwords. However, the company must use one of the alternate methods for releasing call detail information, which are:

- Call the customer at the telephone number of record.
- Send to the address of record (postal or electronic).
- Ask the customer to come into the office and provide a valid photo ID.

Can the company discuss an account with a spouse if they are not listed on the account as an authorized contact?
No

What about people in nursing homes? Can the company discuss the account with a daughter or son of the account holder?
Only if they are listed on the account or they have provided a Power of Attorney authorization.

What if we have an account where the person is deceased? The spouse has not changed the name because the spouse wants the deceased person's name to remain on the account and be listed in the phone book, which happens a lot when the husband passes away.
The company should contact the household to make arrangements to get a living customer's name added to the account. If a person notifies you that a customer has died and asks to have the name changed on the account or the account disconnected, the company should request some type of proof, e.g., death certificate, copy of the obituary.

Are unused minutes of a calling plan considered "call detail" information?
No, so password protection is not required, but the company must still authenticate the customer as required for non-call detail information.

What authentication is required for online accounts?
Password.

Can the username for an e-bill be based on account information as long as the password is not based on biographical or account information?

Yes, the username can be based on biographical or account information. The rules apply only to the password associated with the account.

Can a company use its best cable TV customers to market a phone bundle?
Yes, because cable TV (as long as it's not providing voice) does not fall under the CPNI rules.

Can a company use CPNI from its local or long distance customers to market a cable product?
No, unless it has received approval from the customer to use the customer's CPNI for marketing purposes.

Can a company include marketing articles in a newsletter or include a marketing bill insert even if there are some customers that have opted out?
Yes, because this is "mass" marketing and not selective marketing based on CPNI.

If a customer receives long distance service from another provider for which our company does the billing and collection, can our company use that information to market our long distance? Isn't it OK since it appears on the bill that we provide to the customer?
No, you can only use the customer's CPNI from services that your company provides. The customer would need to give you specific approval to look at the CPNI of their long distance provider.

How long do customer CPNI notifications and requests for approval need to be retained by the company?
A minimum of one year.

Can the notification that must be sent to customers when a change has been made to the account be sent by e-mail?
Yes, if the customer has authorized the company to use e-mail and the e-mail address has been associated with the account for at least 30 days.

Does the company need to send a change notification to a customer if the customer adds or deletes services?
No, the notification is required only when a change has been made to an address, a password, the backup authentication or an online account.

The rules say that subscriber list information is not CPNI when used for publication in a directory. If a directory provider wants subscriber list information only for businesses or only for certain exchanges, can we provide it?
Yes, as long as they are requesting the information for a directory.

DEFINITIONS

Account Information: information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

Address of record: an address, whether postal or electronic, that the carrier has associated with the customer's account for at least 30 days.

Affiliate: a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person. The term "own" means to own an equity interest (or the equivalent thereof) of more than 10 percent.

Aggregate information: collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

Breach: when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

Call detail information: information that pertains to the transmission of specific telephone calls, both inbound and outbound, including number called, number from which calls are received, time, location and duration of calls.

Customer Authentication: Confirmation of the customer's identity, using not-readily-available biographical information.

Customer Proprietary Network Information (CPNI): information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier. The information is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.

Non-call detail information: products, types of services customer subscribes to, technical configuration, amount customer owes, etc.

Opt-in approval: methods for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent after the customer is provided appropriate notification of the carrier's request for consent.

Opt-out approval: methods for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented if the customer has failed to object thereto within the waiting period (min 30 days) after the customer is provided appropriate notification of the carrier's request for consent.

Pretexting: the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records.

Readily available biographical information: social security number or last four digits of that number, customer's mother's maiden name, home address; date of birth.

Subscriber list information: information identifying the listed names, telephone numbers and addresses of subscribers of a carrier when used for publication in a directory and when given to providers of emergency services.

Telephone number of record: the telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

Valid Photo ID: a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

Section 222 of the Telecom Act

SEC. 222. PRIVACY OF CUSTOMER INFORMATION.

(a) IN GENERAL

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) CONFIDENTIALITY OF CARRIER INFORMATION

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION

(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) DISCLOSURE ON REQUEST BY CUSTOMERS

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) AGGREGATE CUSTOMER INFORMATION

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefore.

(d) EXCEPTIONS

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents -

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) -

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) SUBSCRIBER LIST INFORMATION

Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) AUTHORITY TO USE WIRELESS LOCATION INFORMATION

For purposes of subsection (c) (1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to –

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332 (d) of this title), other than in accordance with subsection (d) (4) of this section; or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) SUBSCRIBER LISTED AND UNLISTED INFORMATION FOR EMERGENCY SERVICES

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide information described in subsection (i) (3) (A) (!1) of this section (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers or emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

(h) DEFINITIONS

As used in this section:

(1) CUSTOMER PROPRIETARY NETWORK INFORMATION

The term ‘customer proprietary network information’ means –

(A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications carrier, and that is made

available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

(2) AGGREGATE INFORMATION

The term ‘aggregate customer information’ means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) SUBSCRIBER LIST INFORMATION

The term ‘subscriber list information’ means any information -

(A) identifying the listed names of subscribers or a carrier and such subscribers’ telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(4) PUBLIC SAFETY ANSWERING POINT

The term ‘public safety answering point’ means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) EMERGENCY SERVICES

The term ‘emergency services’ means 9-1-1 emergency services and emergency notification services.

(6) EMERGENCY NOTIFICATION SERVICES

The term ‘emergency notification services’ means services that notify the public of an emergency.

(7) EMERGENCY SUPPORT SERVICES

The term ‘emergency support services’ means information or data base management services used in support of emergency services.

EMPLOYEE CPNI TRAINING CERTIFICATION

On an annual basis an officer of our company must certify to the Federal Communications Commission (FCC) that it has established procedures that are adequate to ensure compliance with the FCC's Customer Proprietary Network Information (CPNI) and Red Flag rules.

One of the things that the officer is certifying to is that employees, especially those that have access to CPNI, have been trained on the CPNI and Red Flag rules. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using for both call detail and non-call detail information.

Our company's policy is to provide the training to all new employees when hired and then on an on-going annual basis, or more frequently, if needed.

By signing below, I acknowledge:

- I have received the required training on the CPNI and Red Flag rules.
- I understand the company's procedures for protecting CPNI and Red Flag.
- I understand the company's disciplinary process if I use CPNI and Red Flag inappropriately.
- I understand that if I have any questions at any time regarding the rules, I should immediately contact the company's CPNI Compliance Officer.

Employee Printed Name: _____

Signature: _____ Date: _____

WITNESSED BY THE CPNI COMPLIANCE OFFICER

Printed Name: _____

Signature: _____ Date: _____

RC COMPLIANCE OFFICER & CONTACT INFORMATION

Compliance Officer:

Wanda Heesch
Billing & Customer Service Manager

Contact Information:

RC Technologies Main Office
205 Main Street * PO Box 197
New Effington, SD 57255

Work: (605) 637-5211
Direct: (605) 637-1015
Fax: (605) 637-5302
e-mail: wheesch@tnics.com

LOCATION OF IMPORTANT DOCUMENTS

CPNI Compliance Manual: Filed under "C", in the vault of RC's Main Office, located at 205 Main St., New Effington, SD.

Annual Corporate Officer Certification Form: Filed under "C", in the vault of RC's Main Office, located at 205 Main St., New Effington, SD.

Employee Annual Certification: Filed under "C", in the third drawer of the fireproof filing cabinet, located in the office of the Compliance Officer.

RC Technologies
205 Main St
PO Box 197
New Effington, SD 57255

I, Scott Bostrom, General Manager, hereby certify the information contained in this Customer Proprietary Network Information Compliance Manual & Operating Procedures is accurate and complete to the best of my knowledge, information and belief.

Signed: _____

Printed Name: _____

Title: _____

Date: _____